

⑫ 公開特許公報(A)

平3-291786

⑤Int.Cl.⁵

識別記号

庁内整理番号

⑬公開 平成3年(1991)12月20日

G 06 K 19/07
B 42 D 15/10

5 2 1

6548-2C
6711-5L

G 06 K 19/00

N

審査請求 未請求 請求項の数 2 (全5頁)

⑭発明の名称 ICカード

⑯特 願 平2-95711

⑰出 願 平2(1990)4月10日

⑱発明者 高 木 伸 哉 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 ⑱発明者 武 藤 義 弘 大阪府門真市大字門真1006番地 松下電器産業株式会社内
 ⑲出 願 人 松下電器産業株式会社 大阪府門真市大字門真1006番地
 ⑳代 理 人 弁理士 栗 野 重 孝 外1名

明 細 書

1. 発明の名称

ICカード

2. 特許請求の範囲

(1) 少なくともCPUと、書換え不可能な第1の不揮発性メモリと、書換え可能な第2の不揮発性メモリとを備え、前記書換え可能な第2の不揮発性メモリが、外部から与えられるコマンドに従った処理を行うためのプログラムを格納する第1の領域と、前記コマンドを識別する情報を格納する第2の領域と、前記第1の領域に関するアドレス情報を格納する第3の領域とを有するICカード。
 (2) 第1の領域に格納されるプログラムは機械語プログラムであり、第1の不揮発性メモリまたは第2の不揮発性メモリが、前記機械語プログラムへの翻訳プログラムを有することを特徴とする請求項1記載のICカード。

3. 発明の詳細な説明

産業上の利用分野

本発明は、CPUとメモリを内蔵するICカー

ドに関する。

従来の技術

ICカードは磁気カードに比べて記憶容量が大きく、また高度なセキュリティ機能を有することにより、次世代のカードとして注目を集め、金融・流通・医療を初めとする多くの分野で実用化実験が行なわれている。従来のICカードは、予め決定された固定のプログラムをマスクROM化するのが一般的であった。

発明が解決しようとする課題

しかし、従来の方法では、プログラムが固定であるため、機能の変更あるいは拡張が困難であった。すなわち新しい機能を追加する場合には、再度マスクROMを起こす必要があった。

また、例えば銀行関連の業務においてICカードを使用する場合、ICカード内部で自動的に残高を更新する等のコマンドを設けることはセキュリティ上極めて好ましいが、このICカードをその他の様々な用途に使用するために、このようなアプリケーション固有のコマンドを設けず、各用途

で共通に使えるコマンドのみを持たせていた。そのため、例えば銀行関連の業務においても前記共通のコマンドの組合せによって各機能を実現する以外に方法はなく、ICカードがCPUを内蔵しているにもかかわらず、十分なセキュリティ機能や高い処理効率を実現するまでには至っていなかった。

本発明はこのような課題に鑑み、各アプリケーションに応じて機能の拡張が容易に行えるICカードを提供することを目的とする。

課題を解決するための手段

この課題を解決するために本発明のICカードは、少なくともCPUと、書換え不可能な第1の不揮発性メモリと、書換え可能な第2の不揮発性メモリとを備え、前記書換え可能な第2の不揮発性メモリが、外部から与えられるコマンドに従った処理を行うためのプログラムを格納する第1の領域と、前記コマンドを識別する情報を格納する第2の領域と、前記第1の領域に関するアドレス情報を格納する第3の領域とを設けたことを特徴

とするものである。

作用

この構成により、新しい機能を実現するプログラムを前記第1の領域に書き込み、外部からのコマンドによって、それを実行させることが可能となるため、各アプリケーションに適した機能をICカードに随時追加できることとなる。

実施例

第1図は、本発明の一実施例によるICカードのブロック図である。第1図において、1はICカードであり、CPU 2、マスクROM 3、EEPROM 4、RAM 5および内部バス6を内蔵している。マスクROM 3は、ICカード1の処理の骨格をなすメインプログラム7と、変更されることのない固定の基本サブルーチン群8を格納している。またRAM 5は、メインプログラム7や後述する複数のコマンド処理ルーチンが共通で使用する基本ワークエリア13と、各コマンド処理ルーチンが自由に使用できる応用ワークエリア14とに分割されている。

-3-

EEPROM 4は、ICカード1に新しい機能を追加する際に更新されるコマンドテーブル9を有している。10、11、12は、それぞれ新しい機能を追加するためにEEPROM 4に書き込まれたRコマンド処理ルーチン、Eコマンド処理ルーチン、Dコマンド処理ルーチンである。また第2図は、メインプログラム7の処理のうち、本発明に関連する基本的な部分を示したフローチャートである。

以下、第1図および第2図に従い、本実施例について説明を行なう。まずカード製造者は、EEPROM 4を初期状態、すなわちコマンドテーブル9やコマンド処理ルーチン10～12が格納されていない状態でICカード1を発行者に出荷する。発行者は、自動的に残高を更新する機能(Rコマンド)、データを暗号化する機能(Eコマンド)、データを復号化する機能(Dコマンド)をICカード1に追加したい場合、それらの機能を実現するプログラム(それぞれRコマンド処理ルーチン10、Eコマンド処理ルーチン11、Dコマ

ンド処理ルーチン12)とコマンドテーブル9とをEEPROM 4に書き込む。この書き込み処理を行なうためのプログラムは基本サブルーチン群8の一部であり、コマンド処理に関して高級言語やアセンブリ言語で記述したものを機械語に翻訳するためのコンパイラあるいはアセンブラを含んでいる。

コマンドテーブル9は、例えば第3図に示すような構成となっている。第3図(a)は、コマンドテーブル9の論理的な構成を示すものであり、コマンドコード31と、その処理ルーチンの先頭アドレス32とがテーブルの形で記述されている。また、第3図(b)は、コマンドテーブル9がEEPROM 4に実際に格納されている物理的な配置を示すものであり、33は書き込まれているコマンド処理ルーチンの数を格納するコマンド数格納部、34はコマンドコード格納部、35は先頭アドレス格納部である。

次に第2図を用いて、メインプログラム7の処理の流れを説明する。まず、CPU 2は外部機器

-4-

-5-

-6-

(図示せず) から1つのコマンドを受信する(ステップ21)。ここでは一例として、データを暗号化する機能(Eコマンド)を受信したものとする。Eコマンドを受信すると、CPU2はコマンドテーブル9を参照し(ステップ22)、Eコマンド処理ルーチン11を呼び出し、それを実行する(ステップ23)。ステップ22とステップ23の処理の具体例を以下に示す。以下の記述において、A~Fはそれぞれ8ビットのレジスタを表わし、例えばCDは16ビットのレジスタペアを表わすものとする。また、レジスタAには外部機器から受信したコマンドコードがセットされているものとする。

```
MOV B, [CMDNUM]    ... [1]
MOV CD, CMDCOD      ... [2]
MOV EF, JMPADR      ... [3]
LOOP: CMP A, [CD]   ... [4]
      JNZ NEXT      ... [5]
      CAL [EF]       ... [6]
      JMP RESP      ... [7]
```

-7-

タペアCDで示されるアドレスに格納されている内容(本実施例の場合は、コマンドコード格納部34の先頭に格納されている'R')とが比較される。[5]では、前記比較結果が一致した場合は次の命令[6]を実行するが、本実施例の場合は一致しないので、ラベルNEXTで示される命令[8]へジャンプする。[8]では、CDの内容がインクリメントされ、コマンドコード格納部34の2番目のコード'E'が格納されるアドレスCMDCOD+1がセットされる。同様に[9]ではレジスタペアEFがインクリメントされ、先頭アドレス格納部35の2番目のアドレス'200'が格納されるアドレスJMPADR+1がセットされる。[10]では、レジスタBの内容すなわちコマンド数を示す数値3がデクリメントされ、数値2となる。[11]により、この結果が0とならない場合は、ラベルLOOPで示される命令[4]へ戻り、同様の処理(第2サイクル)を実行する。すなわち、[4]での比較結果が一致するまで、コマンド数格納部33に格納されて

```
NEXT: INC CD        ... [8]
      INC EF        ... [9]
      DEC B         ... [10]
      JNZ LOOP      ... [11]
RESP:                ... [12]
```

[1]のCMDNUMはコマンド数格納部33のアドレスを示すラベルであり、[CMDNUM]はそこに格納されるデータ(本実施例の場合は数値3)を示す。したがって[1]では、レジスタBに数値3がセットされる。[2]、[3]のCMDCODとJMPADRは、それぞれコマンドコード格納部34と先頭アドレス格納部35の先頭のアドレスを示すラベルであり、レジスタペアCDとEFには、それぞれコマンドコード格納部34の先頭アドレスCMDCOD自身と先頭アドレス格納部35の先頭アドレスJMPADR自身がセットされる。第1サイクルとして、[4]では、レジスタAに格納されている内容すなわち外部機器から受信したコマンドコード(本実施例の場合は、暗号化機能を示す'E')と、レジス

-8-

いる数だけ、このサイクルが繰り返される。

前述したように、次の第2サイクルでは、レジスタペアCDには、コマンドコード格納部34の2番目のコード'E'が格納されるアドレスCMDCOD+1がセットされているため、[4]の比較結果は一致する。したがって[5]により、次の命令[6]へ移る。[6]の命令は、レジスタペアEFで示されるアドレスに格納されているアドレスから始まるサブルーチンをコールすることを示している。前述したように、レジスタペアEFの内容は、先頭アドレス格納部35の2番目のアドレス'200'が格納されるアドレスJMPADR+1がセットされているため、アドレス200で始まるサブルーチン、すなわちEコマンド処理ルーチン11が実行される。ここでRAM5内の情報のうち、Eコマンド処理ルーチン11の実行時に破壊してはならないものは、すべて基本ワークエリア13に格納されている。したがって、Eコマンド処理ルーチン11では、応用ワークエリア14を自由に使用することができる。E

-9-

-10-

コマンド処理ルーチン 11 を終了した後は、命令 [7] に戻り、このループを抜けて、レスポンスを送信するための命令 [12] (ラベル名: RESP) にジャンプする。そして最後に、レスポンスを外部機器に送信する (第 2 図のステップ 24)。

発明の効果

以上のように本発明によれば、書換え可能な揮発性メモリに、外部から与えられるコマンドに従った処理を行うためのプログラムを格納する第 1 の領域と、コマンドを識別する情報を格納する第 2 の領域と、第 1 の領域に関するアドレス情報を格納する第 3 の領域とを設けることにより、容易な構成で、内蔵する CPU の機能を十分に活用し、かつ各アプリケーションに適した機能を IC カードに追加できることとなる。また、これにより、1 種類の IC カードを様々な用途に特化したカードとして使用することが可能となる。

4. 図面の簡単な説明

第 1 図は本発明の一実施例による IC カードの

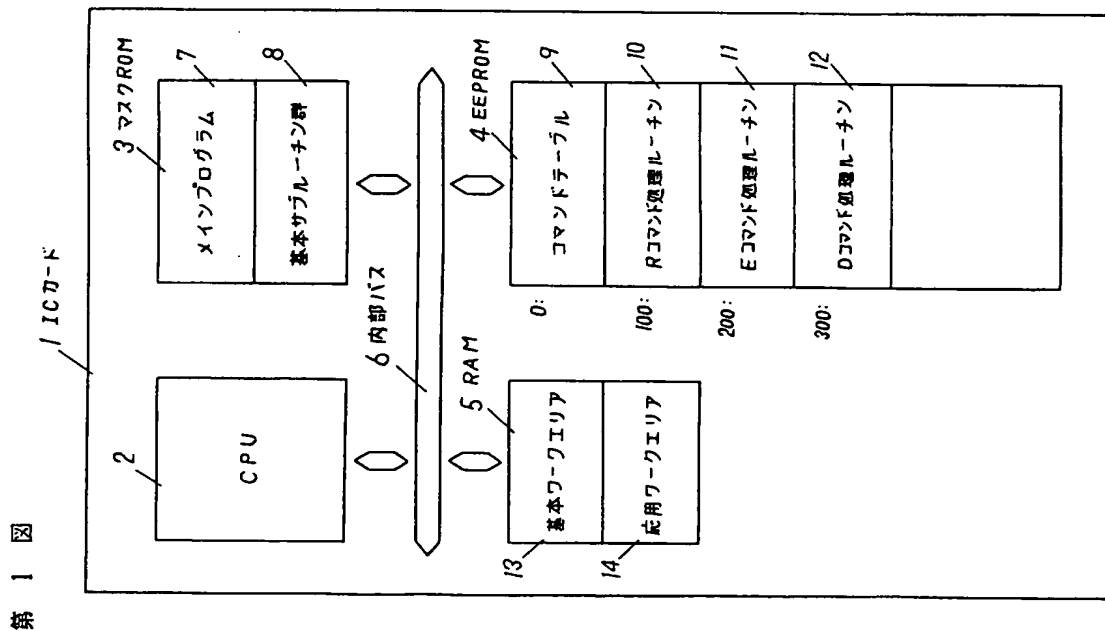
構成を示すブロック図。第 2 図は本発明の一実施例によるメインプログラムのフローチャート、第 3 図 (a) は本発明の一実施例によるコマンドテーブルの論理的構成図、第 3 図 (b) は本発明の一実施例によるコマンドテーブルの物理的構成図である。

1 … IC カード、2 … CPU、3 … マスク ROM、4 … EEPROM、5 … RAM、6 … 内部バス、7 … メインプログラム、8 … 基本サブルーチン、9 … コマンドテーブル、10 … R コマンド処理ルーチン、11 … E コマンド処理ルーチン、12 … D コマンド処理ルーチン。

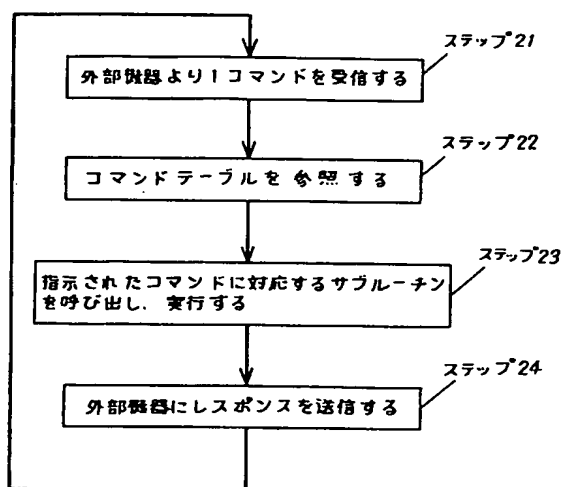
代理人の氏名 弁理士 栗野重孝 ほか 1 名

-11-

-12-



第 2 図



第 3 図

(a)

| 31 コマンドコード | 32 先頭アドレス |
|---------------|--------------|
| R | 100 |
| E | 200 |
| D | 300 |

(b)

